7

Moduluak ideal nagusietako domeinuen gainean

7.1. Modulu finituki sortuen egitura ideal nagusietako domeinu baten gainean

Ezaguna dugu $\varphi : V_1 \longrightarrow V_2$ aplikazio lineal bat definitzeko V_1 eta V_2 bi bektore-espazioren artean (jakina, gorputz beraren gainean), nahikoa dela V_1-en oinarri bateko bektoreen irudiak nahi dugun moduan aukeratzea. Guztiz era beran, emaitza hau dugu modulu aske baten gainean homomorfismoak definitzeko.

7.1. Teorema (Modulu askeen propietate unibertsala)**.** *Izan bitez M_1 eta M_2 bi A-modulu, M_1 askea izanik. Demagun $\{x_i\}_{i\in I}$ M_1-en oinarria dela, eta aukeratu dezagun $\{y_i\}_{i\in I}$ M_2-ko elementuen edozein familia, I indize-multzoarekin indexaturik. Orduan, $x_i \mapsto y_i$ esleipenek $\varphi : M_1 \longrightarrow M_2$ A-moduluen homomorfismo bat, eta bakar bat, definitzen dute. Horren bitartez, $x = \sum_{i\in I} a_i x_i \in M_1$ elementu orokor baten irudia formula honen bitartez emanda dago:*

$$\varphi\Big(\sum_{i\in I} a_i x_i\Big) = \sum_{i\in I} a_i y_i. \tag{7.1}$$

7.2. Korolarioa. *Izan bedi M A-modulu finituki sortua, eta demagun n elementurekin sor daitekeela. Orduan, M A^n-ren zatidura baten isomorfoa da.*

Froga. Izan bedi $\{e_1, \ldots, e_n\}$ A^n-ren oinarri kanonikoa, eta har dezagun n elementu dituen sistema sortzaile bat M-n, $\{y_1, \ldots, y_n\}$. Orduan, $e_i \longmapsto y_i$ erregelak A-moduluen homomorfismo bat definitzen du A^n-tik M-ra. Gainera, (7.1) formularen arabera, φ supraiektiboa da, $\{y_1, \ldots, y_n\}$ M-ren sistema sortzailea izateagatik. Lehenengo isomorfismo-teorema aplikatzen badugu, $M \cong A^n/\ker\varphi$ lortzen dugu, eta M A^n-ren zatidura baten isomorfoa da. □

Zer esan dezakegu A^n modulu askearen azpimoduluei buruz? Horiek ulertzen baditugu, orduan dagozkien zatidura modulu guztiak ere ulertuko ditugu eta, aurreko korolarioaren arabera, modulu finituki sortu guztiak ere bai. Ikusiko dugunez, A ideal nagusietako domeinua denean galdera horri erantzuna eman ahal izango diogu. Hasteko, A^n-ren azpimoduluak finituki sortuak direla ikusiko dugu.

7.3. Proposizioa. *Izan bedi A ideal nagusietako domeinua. Orduan, A^n-ren azpimodulu guztiak finituki sortuak dira, eta gehienez n elementurekin sor daitezke.*

FROGA. Emaitza n-ren gaineko indukzioaz frogatuko dugu. Hasteko, $n = 1$ bada, orduan A-ren azpimoduluak eta idealak bat datoz. Ideal nagusietako domeinua denez, A-ren ideal guztiak elementu bakar baten bidez sor daitezke, eta elementu hori bera sortzailea da azpimodulu gisa.

Orain, demagun emaitza A^{n-1}-en egia dela, eta ikus dezagun A^n-n betetzen dela. Izan bedi N A^n-ren azpimodulua, eta dei diezaiogun Q N-ren proiekzioari azken osagaiaren gainean. Hau da,

$$Q = \{a_n \mid \text{existitzen da } (a_1, \dots, a_n) \text{ elementu bat } N\text{-n}\}.$$

Erraz ikusten da Q A-ren ideala dela. Beraz, $Q = (q)$ dugu $q \in A$ elementu baterako. Har dezagun $x_n \in N$ elementu bat non x_n-ren azken osagaia q baita. Orain, izan bedi

$$N^* = N \cap (A \times \overset{n-1}{\cdots} \times A \times \{0\}) = \{(a_1, \dots, a_{n-1}, a_n) \in N \mid a_n = 0\}.$$

Orduan, N^* A^{n-1}-en azpimodulu baten isomorfoa da eta, indukzio hipotesiagatik, $n-1$ elementurekin sor daiteke: izan bitez $x_1, \dots, x_{n-1}$ elementu horiek.

Ikus dezagun $x_1, \dots, x_n$ N-ren sistema sortzailea dela. Horretarako, aukeratu $x \in N$ edozein. Orduan, x-ren azken osagaia Q-n dago, eta beraz $a_n q$ modukoa da, $a_n \in A$ izanik. Orain, $x^* = x - a_n x_n$ elementua N-n dago, eta haren azken osagaia 0 da. Beraz, $x^* \in N^*$ dugu. Horrela, $x^* = a_1 x_1 + \cdots + a_{n-1} x_{n-1}$ jar dezakegu, $a_i \in A$ izanik. Orduan, $x = a_1 x_1 + \cdots + a_{n-1} x_{n-1} + a_n x_n$ dugu, eta frogaturik dago $\{x_1, \dots, x_n\}$ N-ren sistema sortzailea dela. □

Orain, A^n-ren azpimoduluei buruzko emaitza nagusia enuntziatuko dugu. Hurrengo atalean emango dugu horren froga, matrizeen Smithen forma normala eskura dugunean. Gainera, frogako prozedura bera erabiliko dugu kasu praktikoak ebazteko.

7.4. Teorema. *Izan bedi A ideal nagusietako domeinua, eta demagun N A^n-ren azpimodulua dela. Orduan:*

(i) *N ere A-modulu askea da.*
(ii) *Existitzen dira $\{y_1, \dots, y_m\}$ N-ren oinarri bat ($m \leq n$ izanik) eta $\{x_1, \dots, x_n\}$ A^n-ren oinarri bat non $y_i = d_i x_i$ baita $i = 1, \dots, m$ guztietarako. Gainera, $d_1 \mid d_2 \mid \cdots \mid d_m$ betetzea lor daiteke, eta orduan $d_1, \dots, d_m$ balioak bakarrak dira (unitateez biderkatzea salbu).*

7.5. Definizioa. Izan bitez A ideal nagusietako domeinua eta M A^n-ren azpimodulua. Orduan, 7.4 teoremaren enuntziatuko oinarriak A^n-ren eta N-ren *oinarri egokituak* direla esaten dugu, eta $d_1 \mid d_2 \mid \cdots \mid d_m$ betetzen duten A-ko elementuak N-ren *faktore aldagaitzak* direla esango dugu.

7.6. Korolarioa (Modulu finituki sortuen egitura ideal nagusietako domeinu baten gainean)**.** *Izan bedi A ideal nagusietako domeinua. Demagun M A-modulu finituki sortua dela, n elementurekin sor daitekeena. Orduan,*

$$M \cong \frac{A}{(d_1)} \times \cdots \times \frac{A}{(d_m)} \times A \times \overset{n-m}{\cdots} \times A$$

isomorfismoa dugu $d_1, \ldots, d_m \in A$ elementu batzuetarako. Gainera, $d_1 \mid d_2 \mid \cdots \mid d_m$ betetzea lor daiteke, eta orduan $d_1, \ldots, d_m$ balioak bakarrak dira (unitateez bidekatzea salbu) eta M-ren faktore aldagaitzak *direla esaten dugu.*

Froga. Badakigu, 7.2 korolarioa aplikatuz, $M \cong A^n/N$ isomorfismo bat dagoela, N A^n-ren azpimodulua izanik. Aukeratu ditzagun A^n-ren eta N-ren oinarri egokituak: $\{x_1, \ldots, x_n\}$ eta $\{y_1, \ldots, y_m\}$, hurrenez hurren, non $y_i = d_i x_i$ baita $i = 1, \ldots, m$ guztietarako eta $d_1 \mid d_2 \mid \cdots \mid d_m$ baita. Orain, A^n modulu askearen propietate unibertsala erabiliz, homomorfismo hau definitzen dugu:

$$\begin{array}{rccl}
\varphi \;:\; A^n & \longrightarrow & \dfrac{A}{(d_1)} \times \dfrac{A}{(d_2)} \times \cdots \times \dfrac{A}{(d_m)} \times A \times \overset{n-m}{\cdots} \times A \\
x_1 & \longmapsto & (1 + (d_1), 0 + (d_2), \ldots, 0 + (d_m), 0, \ldots, 0) \\
x_2 & \longmapsto & (0 + (d_1), 1 + (d_2), \ldots, 0 + (d_m), 0, \ldots, 0) \\
\vdots & \vdots & \vdots \\
x_m & \longmapsto & (0 + (d_1), 0 + (d_2), \ldots, 1 + (d_m), 0, \ldots, 0) \\
x_{m+1} & \longmapsto & (0 + (d_1), 0 + (d_2), \ldots, 0 + (d_m), 1, \ldots, 0) \\
\vdots & \vdots & \vdots \\
x_n & \longmapsto & (0 + (d_1), 0 + (d_2), \ldots, 0 + (d_m), 0, \ldots, 1).
\end{array}$$

Orduan, $x \in A^n$ elementu orokor bat $\{x_1, \ldots, x_n\}$ oinarriarekiko idazten badugu, $x = a_1 x_1 + \cdots + a_n x_n$, $a_i \in A$ izanik, hau da x-ren irudia φ-ren bitartez:

$$\varphi(x) = (a_1 + (d_1), a_2 + (d_2), \ldots, a_m + (d_m), a_{m+1}, \ldots, a_n).$$

Horrela, garbi dago φ supraiektiboa dela eta

$$\begin{aligned}
\ker \varphi &= \{a_1 x_1 + \cdots + a_m x_m \mid a_i \in (d_i) \text{ da } i = 1, \ldots, m \text{ guztietarako}\} \\
&= \{b_1 d_1 x_1 + \cdots + b_m d_m x_m \mid b_i \in A \text{ da } i = 1, \ldots, m \text{ guztietarako}\} \\
&= \langle d_1 x_1, \ldots, d_m x_m \rangle = N
\end{aligned}$$

dela. Horrela, lehenengo isomorfismo-teorema aplikatuz,

$$A^n/N \cong \frac{A}{(d_1)} \times \cdots \times \frac{A}{(d_m)} \times A \times \overset{n-m}{\cdots} \times A$$

dugu, eta $M \cong A^n/N$ denez, enuntziatuko isomorfismoa frogaturik gelditzen da. Bakartasunaren froga ez dugu testuliburu honetan aurkeztuko. □

Bereziki, aurreko korolarioa $\mathbb{Z}$-moduluei aplikatzen badiegu, emaitza hau lortzen dugu.

7.7. Teorema (Talde abeldar finituki sortuen egitura)**.** *Izan bedi G talde abeldar finituki sortua, eta ez-tribiala. Orduan, existitzen dira $n_1, \dots, n_k \geq 2$ zenbaki oso bakarrak non $n_1 \mid n_2 \mid \cdots \mid n_k$ baita eta*

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \cong C_{n_1} \times \cdots \times C_{n_k} \times C_\infty \times \cdots \times C_\infty$$

baita.

Froga. Aplikatu 7.6 korolarioa G $\mathbb{Z}$-moduluari. Orduan, d_i guztiak positiboak aukeratu ditzakegu. Kontuan izan $d_i = 1$ balioari dagokion faktorea $\mathbb{Z}/(d_i) = \mathbb{Z}/\mathbb{Z} = \{\overline{0}\}$ dela eta, beraz, faktore hori deskonposiziotik ezaba dezakegula. □

7.2. Matrize baten Smithen forma normala eta oinarri egokituen existentzia

7.8. Lema. *Izan bitez A eraztuna eta M A-modulua. Orduan, M-ren sistema sortzaile bati eraldaketa hauetako bat aplikatzen badiogu, M-ren beste sistema sortzaile bat lortuko dugu:*

(SE1) *Elementuen ordena aldatzea.*
(SE2) *Elementuetako bat unitate batez biderkatzea.*
(SE3) *Elementu bati besteen konbinazio lineal bat batzea.*

Gainera, M modulu askea bada, emaitza bera betetzen da "sistema sortzailea" dagoen tokian "oinarria" jartzen badugu.

Froga. Berehalakoa da; eraztunen idealekin egiten genuen bezala ikus daiteke. □

7.9. Definizioa. Aurreko leman agertzen diren (SE1), (SE2) eta (SE3) eraldaketak *sistema sortzaileen eraldaketa elementalak* direla esaten dugu.

Orain, N A^n-ren azpimodulu finituki sortua bada, C matrize bat egokitu diezaiokegu. Horretarako, hartu $\mathcal{B} = \{w_1, \dots, w_n\}$ A^n-ren oinarria eta $\mathcal{S} = \{z_1, \dots, z_r\}$ N-ren sistema sortzailea, eta jarri z_i elementuen koordenatuak $\mathcal{B}$ oinarriarekiko C matrizearen i. zutabean. Horrela, $C \in M_{n\times r}(A)$ dugu, eta $C = M_{\mathcal{B}}(\mathcal{S})$ idatziko dugu. Zein da eragina C matrizearen gainean $\mathcal{B}$-ri edo $\mathcal{S}$-ri sistema sortzaileen eraldaketa elementalak aplikatzen badizkiegu? Erraz ikus daiteke emaitza hau dugula.

7.10. Proposizioa. *Izan bedi N A^n-ren azpimodulu finituki sortua, har ditzagun $\mathcal{B} = \{w_1, \dots, w_n\}$ A^n-ren oinarria eta $\mathcal{S} = \{z_1, \dots, z_r\}$ N-ren sistema sortzailea, eta jarri $C = M_{\mathcal{B}}(\mathcal{S})$. Orduan:*

(i) *$\mathcal{S}$ sistema sortzaileari (SE1), (SE2) edo (SE3) eraldaketa elementalak aplikatzen badizkiogu, $\mathcal{S}'$ N-ren sistema sortzaile berria lortuz, orduan $M_{\mathcal{B}}(\mathcal{S}')$ matrize berria lortzeko eraldaketa hauetako bat egin behar da C-ren gainean, hurrenez hurren:*
   (ZE1) *Zutabeen ordena aldatzea.*

(ZE2) *Zutabe bat unitate batez biderkatzea.*
(ZE3) *Zutabe bati besteen konbinazio lineal bat batzea.*

(ii) *$\mathcal{B}$ oinarriari (SE1), (SE2) edo (SE3) eraldaketa elementalak aplikatzen badizkiogu, $\mathcal{B}'$ A^n-ren oinarri berria lortuz, orduan $M_{\mathcal{B}'}(\mathcal{S})$ matrize berria lortzeko eraldaketa hauetako bat egin behar da C-ren gainean, hurrenez hurren:*
(EE1) *Errenkaden ordena aldatzea.*
(EE2) *Errenkada bat unitate batez biderkatzea.*
(EE3) *Errenkada bati besteen konbinazio lineal bat batzea.*

Alderantziz ere, $M_{\mathcal{B}}(\mathcal{S})$ matrizeari aurrekoak bezalako aldaketak aplikatzen badizkiogu, orduan $M_{\mathcal{B}'}(\mathcal{S}')$ moduko matrize bat lortzen dugu, $\mathcal{B}'$ A^n-ren oinarria eta $\mathcal{S}'$ N-ren sistema sortzailea izanik.

7.11. Definizioa. Izan bedi C matrizea. Orduan, aurreko proposizioan agertzen diren C matrizearen gaineko (ZE1), (ZE2) eta (ZE3) eraldaketak *zutabeen eraldaketa elementalak* direla esaten dugu, eta (EE1), (EE2) eta (EE3), berriz, *errenkaden eraldaketa elementalak*.

Orain, 7.4 teoremako oinarri egokituak lortzeko giltza ondorengo emaitzak ematen digu.

7.12. Teorema. *Izan bitez A ideal nagusietako domeinua eta $A \in M_{n\times r}(C)$. Orduan, C matrizeari errenkaden eta zutabeen eraldaketa elementalak eginez, hau bezalako matrize batera irits gaitezke:*

$$D = \begin{pmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & d_m & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Gainera, $d_1 \mid d_2 \mid \cdots \mid d_m$ izatea lor dezakegu, eta baldintza hori bete behar badute, d_i elementuak bakarrak dira, unitateez biderkatzea salbu. Horiek C matrizearen faktore aldagaitzak *direla esaten dugu, eta D matrizeari C-ren* Smithen forma normala *deitzen zaio.*

Froga. Bakartasuna ez dugu testuliburu honetan frogatuko, beraz Smithen forma normalaren existentzian zentratuko gara. Horren froga eraikikorra da, eta D matrizea lortzeko algoritmo bat emango dugu. Erraztasunez, domeinu euklidear baten kasuan baino ez dugu emango algoritmo hori. Praktikan erabiliko ditugun kasuak $A = \mathbb{Z}$-rena eta $A = K[X]$-rena izango dira (K gorputza izanik), eta biak domeinu euklidearrak direnez, orain emango dugun metodoak bi kasu horietarako balioko du.

Jakina, C matrize nulua bada, orduan $D = C$ dugu. Beraz, C-k elementu ez-nuluak dituen kasuan jar gaitezke. Smithen forma normala lortzeko, nahikoa da jakitea nola pasatu, eraldaketa elementalak erabiliz, C matrizetik

$$C^* = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & c^*_{22} & \cdots & c^*_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c^*_{n2} & \cdots & c^*_{nn} \end{pmatrix}$$

moduko matrize batera, non $d_1 \mid c^*_{ij}$ baita $2 \leq i, j \leq n$ guztietarako. Oinarrizko pauso hori egiten badakigu, orduan prozedura errepikatuko dugu lehenengo errenkada eta zutabea ezabatuz lortzen den $(n-1) \times (n-1)$ tamainako matrizearekin, eta horrela jarraituz, azkenean D matrizea lortuko dugu.

Azaldu dezagun, orduan, nola lor daitekeen C^*-era pasatzea. Pauso hauek jarraituko ditugu:

(SM1) Aukeratu C matrizean φ funtzio euklidearraren balio minimoa duen elementu ez-nulu bat. (Orduan, $A = \mathbb{Z}$ bada, balio absolutu txikieneko elementu bat aukeratuko dugu, eta $A = K[X]$ bada, maila txikieneko polinomio bat.) Elementu hori matrizearen $(1,1)$ posiziora eramango dugu errenkadak edo/eta zutabeak elkarrekin aldatuz.

(SM2) $(1,1)$ posizioan dagoen c_{11} elementu berriak matrizearen beste sarrera guztiak zatitzen baditu, orduan zeroak egingo ditugu lehenengo zutabean (errenkada bakoitzari lehenengo errenkadaren multiplo bat kenduz) eta lehenengo errenkadan (zutabe bakoitzari lehenengo zutabearen multiplo bat kenduz). Hori egin eta gero, oraindik ere matrize berriaren sarrera guztiak zatitzen ditu c_{11}-ek. Beraz, C^* matrizea lortu dugu dagoeneko.

(SM3) $(1,1)$ posizioan dagoen c_{11} elementu berriak ez baditu matrizearen sarrera guztiak zatitzen, orduan zatitzen ez duen c_{ij} elementu bat aukeratuko dugu. Jarraitzeko modua desberdina da c_{ij}-ren posizioaren arabera.

(SM3-a) Demagun $i = 1$ dela, hau da, c_{11}-ek zatitzen ez duen elementua lehenengo errenkadan aukeratu daitekeela. Orduan, c_{1j} c_{11}-ez zatituz, $c_{1j} = qc_{11} + r$ dugu, $r \neq 0$ izanik. Biderkatzen badugu lehenengo zutabea q-rekin eta j. zutabeari kentzen badiogu, orduan $(1,j)$ posizioan r agertuko da. Orain, $\varphi(r) < \varphi(c_{11})$ denez, gure matrizean funtzio euklidearraren balio txikiago bat duen elementu bat lortu dugu, eta (SM1) kasura itzuliko gara.

(SM3-b) Demagun $j = 1$ dela, hau da, c_{11}-ek zatitzen ez duen elementua lehenengo zutabean aukeratu daitekeela. Orduan, aurreko kasuan bezala jokatuko dugu φ-ren balio txikiago bat duen elementu bat lortzeko, baina errenkadak erabiliz.

(SM3-c) Demagun $i, j \geq 2$ dela nahitaez, hau da, lehenengo errenkadako eta lehenengo zutabeko elementu guztiak c_{11}-en multiploak direla, eta zatigarria ez den elementua $\{2, \ldots, n\}$ indizeei dagokien $(n-1)\times(n-1)$ tamainako matrizean dagoela. Orduan, c_{i1} elementua c_{11}-en berdina

bihurtuko dugu: $c_{i1} = qc_{11}$ bada, kendu i. errenkadari lehenengoa bider $q-1$. Orduan, (SM3-a) kasuan bezala, (i,j) posizioan φ-ren balio txikiagoa duen elementu bat lortuko dugu.

Aurreko prozedura benetan algoritmo bat izateko, ziurtatu behar dugu amaiatu egiten dela. Beraz, argitu behar dugu zergatik ezin garen erori bukle infinitu batean, behin eta berriz (SM1) hasierako pausora itzuliz. Gakoa da φ funtzio euklidearrak $\mathbb{N} \cup \{0\}$ multzoan hartzen dituela balioak. Konturatzen bagara (SM1) pausora itzultzen garen bakoitzean matrizeko elementu ez-nuluen φ-ren balio minimoa jaitsi egiten dela, orduan garbi dago bukle infinitu hori ezinezkoa dela. □

7.13. Adibidea. Kalkula dezagun

$$C = \begin{pmatrix} 6 & 10 & 0 \\ 6 & 0 & 15 \\ 0 & 10 & 15 \end{pmatrix}$$

matrizearen Smithen forma normala, eraldaketa elementalak aplikatuz.

$$C \xrightarrow{Z_2 \to Z_2 - Z_1} \begin{pmatrix} 6 & 4 & 0 \\ 6 & -6 & 15 \\ 0 & 10 & 15 \end{pmatrix} \xrightarrow{Z_1 \leftrightarrow Z_2} \begin{pmatrix} 4 & 6 & 0 \\ -6 & 6 & 15 \\ 10 & 0 & 15 \end{pmatrix}$$

$$\xrightarrow{Z_2 \to Z_2 - Z_1} \begin{pmatrix} 4 & 2 & 0 \\ -6 & 12 & 15 \\ 10 & -10 & 15 \end{pmatrix} \xrightarrow{Z_1 \leftrightarrow Z_2} \begin{pmatrix} 2 & 4 & 0 \\ 12 & -6 & 15 \\ -10 & 10 & 15 \end{pmatrix}$$

$$\xrightarrow{E_2 \to E_2 - 5E_1} \begin{pmatrix} 2 & 4 & 0 \\ 2 & -26 & 15 \\ -10 & 10 & 15 \end{pmatrix} \xrightarrow[(15 = 7 \cdot 2 + 1 \text{ baita})]{Z_3 \to Z_3 - 7Z_1} \begin{pmatrix} 2 & 4 & -14 \\ 2 & -26 & 1 \\ -10 & 10 & 85 \end{pmatrix}$$

$$\xrightarrow{E_1 \leftrightarrow E_2} \begin{pmatrix} 2 & -26 & 1 \\ 2 & 4 & -14 \\ -10 & 10 & 85 \end{pmatrix} \xrightarrow{Z_1 \leftrightarrow Z_3} \begin{pmatrix} 1 & -26 & 2 \\ -14 & 4 & 2 \\ 85 & 10 & -10 \end{pmatrix}$$

$$\xrightarrow[Z_3 \to Z_3 - 2Z_1]{Z_2 \to Z_2 + 26Z_1} \begin{pmatrix} 1 & 0 & 0 \\ -14 & -360 & 30 \\ 85 & 2220 & -180 \end{pmatrix} \xrightarrow[E_3 \to E_3 - 85E_1]{E_2 \to E_2 + 14E_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -360 & 30 \\ 0 & 2220 & -180 \end{pmatrix}$$

$$\xrightarrow{Z_2 \leftrightarrow Z_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 30 & -360 \\ 0 & -180 & 2220 \end{pmatrix} \xrightarrow{Z_3 \to Z_3 + 12Z_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 30 & 0 \\ 0 & -180 & 60 \end{pmatrix}$$

$$\xrightarrow{E_3\to E_3+6E_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 30 & 0 \\ 0 & 0 & 60 \end{pmatrix} = D.$$

Horrenbestez, C matrizearen Smithen forma normala lortu dugu; bereziki, C-ren faktore aldagaitzak 1, 30 eta 60 dira.

7.14. Oharra. Aljebra linealean gertatzen den bezala, C matrize baten gainean (ZE1), (ZE2), (ZE3), (EE1), (EE2) edo (EE3) bezalako eraldaketa elemental bat egiten dugunean, ikus daiteke emaitza bera lortzen dela matrize egoki batez biderkatuz. Gainera, matrize horien determinantea A-ren unitate bat dela ikus daiteke. Hori dela eta, C matrizearen Smithen forma normala D bada, orduan $\det D = u \det C$ dugu, $u \in A^\times$ izanik. Propietate hori Smithen forma normalaren kalkulua bukatutakoan erabil daiteke, egiaztapen modura: akatsak detektatzeko balio dezake, determinanteen arteko diferentzia ez bada unitate bat, baina kontrako kasuan ez du ziurtatzen kalkulua ondo eginda dagoenik. Azken adibidean, $\det C = -1800$ eta $\det D = 1800$ dugu. Bien arteko diferentzia $-1 \in \mathbb{Z}^\times$ da, eta ez dugu akatsik detektatzen.

7.15. Korolarioa. *Izan bedi A ideal nagusietako domeinua, eta demagun N A^n-ren azpimodulua dela. Orduan existitzen dira $\{y_1, \dots, y_m\}$ N-ren oinarri bat ($m \leq n$ izanik) eta $\{x_1, \dots, x_n\}$ A^n-ren oinarri bat non $y_i = d_i x_i$ baita $i = 1, \dots, m$ guztietarako. Gainera, $d_1 \mid d_2 \mid \cdots \mid d_m$ betetzea lor daiteke, eta orduan $d_1, \dots, d_m$ balioak bakarrak dira (unitateez biderkatzea salbu).*

Froga. Badakigu, 7.3 proposizioaren arabera, N finituki sortua dela. Har ditzagun $\mathcal{S} = \{z_1, \dots, z_r\}$ N-ren sistema sortzailea eta $\mathcal{B} = \{e_1, \dots, e_n\}$ A^n-ren oinarri kanonikoa. Jarri $C = M_{\mathcal{B}}(\mathcal{S})$ eta aplika diezaiogun 7.12 teorema C matrizeari. Orain, D matrizea C-ri eraldaketa elementalak aplikatuz lortzen da, eta orduan 7.10 proposizioaren arabera, eraldaketa elemental bakoitza aplikatzen dugunean, lortzen dugun matrize berria $M_{\mathcal{B}'}(\mathcal{S}')$ moduko matrize bat da, $\mathcal{S}'$ oraindik ere N-ren sistema sortzailea izanik, eta $\mathcal{B}'$ A^n-ren oinarria izanik. Beraz, D matrizea ere $M_{\mathcal{B}'}(\mathcal{S}')$ moduko matrize bat da eta, orduan, $\mathcal{S}' = \{y_1, \dots, y_m\}$ eta $\mathcal{B}' = \{x_1, \dots, x_n\}$ jartzen badugu, enuntziatuko baldintzak betetzen dira. (Ohartu $\mathcal{S}'$ N-ren sistema sortzailea oinarria dela benetan; izan ere, linealki independentea da bere elementuak $\mathcal{B}'$ oinarrikoen multiploak direlako eta A integritate-domeinua delako.) □

Ikus dezagun nola erabil dezakegun Smithen forma normala $\mathbb{Z}$-ren gainean talde abeldar finituki sortu baten egitura emateko, sortzaileen eta erlazioen bidez emanda badago.

7.16. Adibidea. Izan bedi $G = \langle a, b, c \rangle$ erlazio hauek betetzen dituen talde abeldarra:

$$a^{-7}b^2c^{-4} = a^{-16}b^5c^{-7} = a^9b^{-3}c^3 = 1.$$

Adieraz dezagun G talde ziklikoen biderkadura zuzen gisa.

Lehenengo eta behin, G taldearen eragiketaren notazioa aldatuko dugu, biderketaren ordez batuketa erabiliz. Horrela, $G = \langle a, b, c\rangle$ dugu, eta erlazio hauek betetzen dira:

$$-7a + 2b - 4c = -16a + 5b - 7c = 9a - 3b + 3c = 0. \tag{7.2}$$

Orain, G talde abeldarra izategatik, $\mathbb{Z}$-modulua da. Hiru sortzaile dituenez, $\mathbb{Z}^3$-ren zatidura baten isomorfoa da. Hau da, $G \cong \mathbb{Z}^3/N$ dugu $\mathbb{Z}^3$-ren N azpimoduluren batentzat.

Zehazkiago, $\mathbb{Z}^3$ $\mathbb{Z}$-modulu askea denez, orduan $\mathcal{B} = \{e_1, e_2, e_3\}$ oinarri kanonikoa hartuta, modulu-homomorfismo hau defini dezakegu oinarriko bektoreen irudiak baino ez emanez:

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}^3 & \longrightarrow & G \\ & & e_1 & \longmapsto & a \\ & & e_2 & \longmapsto & b \\ & & e_3 & \longmapsto & c. \end{array}$$

Orduan,

$$\begin{aligned} \varphi(x, y, z) &= \varphi(xe_1 + ye_2 + ze_3) \\ &= x\varphi(e_1) + y\varphi(e_2) + z\varphi(e_3) = xa + yb + zc \end{aligned} \tag{7.3}$$

dugu $(x, y, z) \in \mathbb{Z}^3$ guztietarako. Hemendik φ supraiektiboa dela ondorioztatzen dugu. Bestalde, (7.2)-ko definizio-erlazioek esaten digute

$$\varphi(-7, 2, -4) = \varphi(-16, 5, -7) = \varphi(9, -3, 3) = 0$$

dela eta, hortaz,

$$(-7, 2, -4),\ (-16, 5, -7),\ (9, -3, 3) \in \ker \varphi.$$

Orain, definizio-erlazioen esanahiaren arabera, a, b eta c elementuen konbinazio lineal batek 0 balio du baldin eta soilik baldin erlazio horien konbinazio bat bada. Horrek esan nahi du, zehatz-mehatz,

$$\ker \varphi = \langle (-7, 2, -4), (-16, 5, -7), (9, -3, 3)\rangle$$

dela. Lehenengo isomorfismo-teorema aplikatuz, $G \cong \mathbb{Z}^3/N$ lortzen dugu,

$$N = \langle (-7, 2, -4), (-16, 5, -7), (9, -3, 3)\rangle$$

izanik. Horrela, esplizitua egin dugu hasieran esan duguna: G taldea $\mathbb{Z}^3$-ren zatidura baten isomorfoa dela.

Orain, ideal nagusietako domeinuen gaineko moduluen teoria aplikatuko dugu. Horretarako, N-ren $\mathcal{S} = \{(-7, 2, -4), (-16, 5, -7), (9, -3, 3)\}$ sistema sortzaileari eta $\mathbb{Z}^3$-ren $\mathcal{B}$ oinarri kanonikoari dagokien $C = M_{\mathcal{B}}(\mathcal{S})$ matrizea hartuko dugu:

$$C = \begin{pmatrix} -7 & -16 & 9 \\ 2 & 5 & -3 \\ -4 & -7 & 3 \end{pmatrix}.$$

Orain, C matrizearen Smithen forma normala kalkulatuko dugu, eraldaketa elementalak aplikatuz:

$$C \xrightarrow{E_1\to E_1+4E_2} \begin{pmatrix} 1 & 4 & -3 \\ 2 & 5 & -3 \\ -4 & -7 & 3 \end{pmatrix} \xrightarrow[Z_3\to Z_3+3Z_1]{Z_2\to Z_2-4Z_1} \begin{pmatrix} 1 & 0 & 0 \\ 2 & -3 & 3 \\ -4 & 9 & -9 \end{pmatrix}$$

$$\xrightarrow[E_3\to E_3+4E_1]{E_2\to E_2-2E_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 3 \\ 0 & 9 & -9 \end{pmatrix} \xrightarrow{Z_3\to Z_3+Z_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 9 & 0 \end{pmatrix}$$

$$\xrightarrow{E_3\to E_3+3E_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{E_2\to -E_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix} = D.$$

Zein interpretazio du D matrizeak? Galdera horri erantzuteko, gogoratu zein den eraldaketa elementalen efektua N moduluari dagokionez:

(a) Zutabeetako eraldaketa bat egiten dugunean, N-ren sortzaileak aldatzen ari gara.
(b) Errenkadetako eraldaketa bat egiten dugunean, $\mathbb{Z}^3$-ren oinarria aldatzen ari gara.

Ondorioz, badaude $\mathcal{B}' = \{x_1, x_2, x_3\}$ $\mathbb{Z}^3$-ren oinarri bat eta $\mathcal{S}' = \{y_1, y_2, y_3\}$ N-ren sistema sortzaile bat, non $M_{\mathcal{B}'}(\mathcal{S}') = D$ baita. Hau da,

$$\begin{cases} y_1 = x_1 \\ y_2 = 3x_2 \\ y_3 = 0 \end{cases}$$

dugu. Teorian ikusi genuen bezala, hemendik isomorfismo hau ondorioztatzen da:

$$\frac{\mathbb{Z}^3}{N} \cong \frac{\mathbb{Z}}{(1)} \times \frac{\mathbb{Z}}{(3)} \times \frac{\mathbb{Z}}{(0)} = \frac{\mathbb{Z}}{\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{\{0\}} \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \mathbb{Z},$$

$\mathbb{Z}/\mathbb{Z} = \{\bar{0}\}$ eta $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ baita. Beraz,

$$G \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \mathbb{Z} \cong C_3 \times C_\infty$$

isomorfismoa dugu, eta lortu dugu G talde abeldarra talde ziklikoen biderkadura zuzen gisa adieraztea.

7.3. Aplikazioa: endomorfismoen forma kanoniko arrazionala

7.17. Teorema. *Izan bedi V bektore-espazioa K gorputzaren gainean,* $\dim V = n$ *izanik. Demagun $\varphi : V \longrightarrow V$ aplikazio lineala dela, eta ikus dezagun V $K[X]$-modulu gisa φ erabiliz. Orduan, $C \in M_n(K)$ φ-ri elkartutako matrize bat bada,*

$$V \cong K[X]^n/N$$

$K[X]$-moduluen isomorfismoa dugu,

$$N = \langle (X - c_{11}, -c_{21}, \ldots, -c_{n1}), (-c_{12}, X - c_{22}, \ldots, -c_{n2}), \ldots, (-c_{1n}, -c_{2n}, \ldots, X - c_{nn}) \rangle$$

izanik.

Froga. Izan bedi $\mathcal{B} = \{v_1, \ldots, v_n\}$ V-ren oinarria non $M_{\mathcal{B}}(\varphi) = C$ baita. Orduan, $\{e_1, \ldots, e_n\}$ $K[X]^n$-ren oinarri kanonikoa bada, $\Phi : K[X]^n \longrightarrow V$ modulu-homomorfismo bat defini dezakegu $\Phi(e_i) = v_i$ erregelaren bitartez. Argi eta garbi, Φ supraiektiboa da. Beraz, lehenengo isomorfismo-teoremaren arabera, $K[X]^n/N \cong V$ isomorfismoa lortzeko nahikoa izango da $\ker \Phi = N$ dela frogatzea.

Ohartu

$$\Phi(0, \overset{i-1}{\ldots}, 0, X, 0, \overset{n-i}{\ldots}, 0) = \Phi(Xe_i) = X\Phi(e_i) = Xv_i = \varphi(v_i)$$

dela eta, ondorioz,

$$\Phi(f_1(X), \ldots, f_n(X)) = f_1(\varphi)(v_1) + \cdots + f_n(\varphi)(v_n)$$

dugula $f_1(X), \ldots, f_n(X) \in K[X]$ guztietarako. Bereziki,

$$\Phi(X - c_{11}, -c_{21}, \ldots, -c_{n1}) = \varphi(v_1) - c_{11}v_1 - c_{21}v_2 - \cdots - c_{n1}v_n = 0,$$

matrize elkartuaren definizioa erabiliz. Antzera ikusten da Φ-k N-ren beste sortzaileak ere 0ra eramaten dituela. Beraz, $N \leq \ker \Phi$ dugu.

Bestalde, $K[X]/\ker \Phi \cong V$ $K[X]$-moduluen isomorfismoa betetzen denez, bereziki $K[X]/\ker \Phi$ eta V bektore-espazio isomorfoak dira K gorputzaren gainean. Hortaz, $\dim K[X]/\ker \Phi = \dim V = n$ dugu. Ikusten badugu $\dim K[X]/N \leq n$ dela, orduan $N \leq \ker \Phi$ izateagatik, zuzenean ondorioztatuko dugu $\ker \Phi = N$ berdintza.

Frogatu dezagun, bada, $\dim K[X]^n/N \leq n$ dela. Lehenengo eta behin, ohartu

$$(0, \overset{i-1}{\ldots}, 0, X, 0, \overset{n-i}{\ldots}, 0) \equiv (c_{1i}, \ldots, c_{i-1,i}, c_{ii}, c_{i+1,i}, \ldots, c_{ni}) \pmod{N} \tag{7.4}$$

dela,

$$(-c_{1i}, \ldots, -c_{i-1,i}, X - c_{ii}, -c_{i+1,i}, \ldots, -c_{ni}) \in N$$

da eta. Kontuan izan, N $K[X]$-azpimodulua izateagatik, kongruentziak elkarrekin batu daitezkeela eta polinomioekin (bereziki K gorputzeko konstanteekin) biderka daitezkeela. Orduan, polinomioen maila maximoaren gaineko indukzioaz argudiatuz, berehala ondorioztatzen da (7.4) kongruentziatik $(f_1(X), \ldots, f_n(X)) \in K[X]^n$ bakoitzeko badagoela $(\lambda_1, \ldots, \lambda_n) \in K^n$ halakoa non

$$(f_1(X), \ldots, f_n(X)) \equiv (\lambda_1, \ldots, \lambda_n) \pmod{N}$$

baita, hau da, non

$$\overline{(f_1(X), \ldots, f_n(X))} = \overline{(\lambda_1, \ldots, \lambda_n)}$$

baita $K[X]^n/N$ zatiduran. Ondorioz,

$$\{\overline{(1, 0, \ldots, 0)}, \overline{(0, 1, \ldots, 0)}, \ldots, \overline{(0, 0, \ldots, 1)}\}$$

$K[X]^n/N$-ren sistema sortzailea izango da K-ren gaineko bektore-espazio gisa, eta horrela $\dim K[X]^n/N \leq n$ desberdintza frogaturik gelditzen da, nahi bezala. □

7.18. Korolarioa. *Aurreko teoremaren baldintzetan, V-ren faktore aldagaitzak eta $XI_n - C \in M_n(K[X])$ matrizearen faktore aldagaitzak bat datoz. Hau da, $XI_n - C$ matrizearen Smithen forma normala*

$$\begin{pmatrix} f_1(X) & 0 & \cdots & 0 \\ 0 & f_2(X) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f_n(X) \end{pmatrix}$$

bada, orduan $K[X]$-moduluen isomorfismo hau dugu:

$$V \cong \frac{K[X]}{(f_1(X))} \times \frac{K[X]}{(f_2(X))} \times \cdots \times \frac{K[X]}{(f_n(X))}. \tag{7.5}$$

Froga. Aplika diezaiogun V $K[X]$-moduluari teorian azaldutako metodo orokorra modulu finituki sortu baten egitura lortzeko ideal nagusietako domeinu baten gainean. Gogoratu hauek direla jarraitu beharreko pausoak:

(i) Adierazi $V \cong K[X]^n/N$ moduan.
(ii) Identifikatu N-ren sistema sortzaile bat eta eraiki matrize elkartu bat, sortzaileen koordenatuak erabiliz.
(iii) Egin eraldaketa elementalak matrize horren gainean, eta lortu dagokion Smithen forma normala.
(iv) Smithen formak N-ren eta $K[X]^n$-ren oinarri egokituen existentzia ziurtatzen du, eta hortik V moduluaren deskonposizioa lor dezakegu, $K[X]$-ren zatidura moduluen biderkadura zuzen gisa.

Aurreko teoreman N-ren sortzaileak eman ditugu,

$$(X - c_{11}, -c_{21}, \ldots, -c_{n1}), (-c_{12}, X - c_{22}, \ldots, -c_{n2}), \ldots, \\ (-c_{1n}, -c_{2n}, \ldots, X - c_{nn})$$

tuplak, alegia. Zutabeka jartzen baditugu tupla horien koordenatuak $K[X]^n$-ren oinarri kanonikoarekiko, orduan $XI_n - C$ matrizea lortzen dugu. Hori dela eta, $XI_n - C$ matrizeak eta V moduluak faktore aldagaitz berberak dituzte. □

7.19. Oharrak. 1) Aurreko korolarioan, $f_1(X), \ldots, f_n(X)$ faktore aldagaitzetatik bat ere ezin da 0 izan. Hala balitz, orduan V-ren deskonposizioan $K[X]/\{0\} \cong K[X]$ faktorea agertuko litzateke. Baina $\dim K[X] = \infty$ dugu, $\dim V = n < \infty$ den bitartean. Hori kontraesana da.

2) Beste alde batetik, $f_i(X)$ polinomioren bat konstante ez-nulua izan daiteke. Orduan, $(f_i(X)) = K[X]$ dugu eta $K[X]/(f_i(X)) = \{\overline{0}\}$ modulu tribiala da. Faktore horiek (7.5) deskonposiziotik ezaba daitezke.

3) Smithen forma normalaren kalkuluan, eraldaketa elemental bat egiten dugun bakoitzean matrize alderanzgarri batez biderkatzen ari gara, eskuinaldetik edo

ezkerraldetik. Beraz, ari garen kasuan

$$XI_n - C = P \begin{pmatrix} f_1(X) & 0 & \cdots & 0 \\ 0 & f_2(X) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f_n(X) \end{pmatrix} Q \tag{7.6}$$

dugu, $P, Q \in GL_n(K[X])$ izanik. Orduan, $\det P$ eta $\det Q$ unitateak izan behar dute $K[X]$-n, hau da, konstante ez-nuluak izan behar dute. Horrela, (7.6) berdintzan determinanteak hartuz,

$$\det(XI_n - C) = \lambda f_1(X) \dots f_n(X)$$

lortzen dugu, $\lambda \in K^\times$ izanik. Gogoratu $\det(XI_n - C)$ φ-ren polinomio karakteristikoa dela, eta $\chi_\varphi(X)$ ikurraz adierazten dugula. Hori n. mailako polinomio monikoa da. Beraz, *faktore aldagaitzak monikoak aukeratzen baditugu*, orduan

$$\chi_\varphi(X) = f_1(X) \dots f_n(X)$$

berdintza dugu, hau da, *faktore aldagaitzen biderkadura polinomio karakteristikoa* da.

Ikusi dugunez, V-ren (7.5) deskonposizioa lortzeko, φ-ri elkartutako matrize bat erabili behar dugu. Segidan ikusiko dugun bezala, prozedurari buelta eman diezaiokegu, eta (7.5) erabil dezakegu φ-ri elkartutako matrize kanoniko bat lortzeko. Horretarako, gogoratu behar dugu modulu kopuru finitu baten biderkadura cartesiarra eta azpimodulu kopuru finitu baten batura zuzena elkarrekin lotuta daudela: horrela, (7.5) biderkadura cartesiarrak

$$V = U_1 \oplus \cdots \oplus U_n$$

batura zuzen gisako deskonposizio bat ematen du. Hemen, U_i bakoitza V-ren $K[X]$-azpimodulu bat da, hau da, azpiespazio φ-aldagaitz bat, eta gainera $U_i \cong K[X]/(f_i(X))$ dugu. Eraikitzen badugu V-ren $\mathcal{B}$ oinarri bat U_i azpiespazioen $\mathcal{B}_i$ oinarriak bilduz, orduan ezaguna da $M_\mathcal{B}(\varphi)$ matrize elkartua blokeka diagonala dela, blokeak U_i azpiespazioetako murrizketen matrizeak izanik:

$$M_\mathcal{B}(\varphi) = \begin{pmatrix} M_{\mathcal{B}_1}(\varphi_{|U_1}) & 0 & \cdots & 0 \\ 0 & M_{\mathcal{B}_2}(\varphi_{|U_2}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_{\mathcal{B}_n}(\varphi_{|U_n}) \end{pmatrix}$$

Orain, bloke horiek nolakoak diren aztertuko dugu. Horretarako, funtsezkoa da hurrengo definizioa.

7.20. Definizioa. Izan bedi $f(X) = X^m + c_{m-1}X^{m-1} + \cdots + c_1X + c_0 \in K[X]$ polinomio monikoa. Orduan, f-ren *matrize laguna* $m \times m$ tamainako matrize hau

da:

$$C(f) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{m-1} \end{pmatrix}.$$

7.21. Lema. *Demagun U V-ren azpiespazioa $K[X]/(f(X))$ zatidurarekin elkartuta dagoela (7.5) isomorfismoaren bitartez, $f(X)$ monikoa eta ez-konstantea izanik. Orduan, U-k badu $\mathcal{C}$ oinarri bat halakoa non $M_{\mathcal{C}}(\varphi_{|U}) = C(f)$ baita.*

Froga. Idatz dezagun $f(X) = X^m + c_{m-1}X^{m-1} + \cdots + c_1X + c_0$. Ezaguna da $\{\overline{1}, \overline{X}, \ldots, \overline{X^{m-1}}\}$ multzoa $K[X]/(f(X))$ zatiduraren oinarria dela, K-ren gaineko bektore-espazio gisa. Orain, (7.5) modulu-isomorfismoa denez, $u \in U$ baldin bada $\overline{1}$-rekin lotuta dagoen elementua, orduan $\{u, Xu, \ldots, X^{m-1}u\}$ U-ren oinarria da. Kontuan hartzen badugu V $K[X]$-moduluan X-rekin biderkatzea φ aplikatzea besterik ez dela, $\mathcal{C} = \{u, \varphi(u), \ldots, \varphi^{m-1}(u)\}$ U-ren oinarria dela lortzen dugu. Gainera, $\overline{f(X)} = \overline{0}$ izateagatik, $f(\varphi)(u) = 0$ dugu, hau da,

$$\varphi^m(u) = -c_0u - c_1\varphi(u) - \cdots - c_{m-1}\varphi^{m-1}(u).$$

Datu horietatik, momentuan lortzen da $M_{\mathcal{C}}(\varphi_{|U}) = C(f)$ berdintza. □

Aurreko guztia erabiliz, hurrengo emaitza hau berehalakoa da.

7.22. Teorema. *Izan bitez V bektore-espazioa K gorputzaren gainean, eta $\varphi : V \longrightarrow V$ aplikazio lineala. Orduan, V-ren faktore aldagaitzak $f_1(X) \mid \cdots \mid f_n(X)$ baldin badira, polinomio horiek moniko hartuta, matrize hau f-ri elkartuta dago:*

$$\begin{pmatrix} C(f_1) & 0 & \cdots & 0 \\ 0 & C(f_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C(f_n) \end{pmatrix}. \tag{7.7}$$

(Hemen, $C(f_i)$ blokea ez da benetan agertzen $f_i(X)$ polinomioa konstantea bada.) Gainera, hori da φ-ri elkartuta dagoen itxura horretako matrize bakarra.

7.23. Definizioa. Aurreko teoreman agertzen den (7.7) matrizeari φ-ren *forma kanoniko arrazionala* deitzen zaio.

7.24. Adibidea. Izan bedi $\varphi : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ endomorfismoa,

$$\varphi(x, y, z) = (x + z, -y - z, -x + y)$$

formularen bidez emanda. Kalkula dezagun φ-ren forma kanoniko arrazionala.

Lehenengo eta behin, φ-ren matrizea kalkulatzen dugu $\mathbb{R}^3$-ren oinarri kanonikoarekiko:

$$C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & -1 \\ -1 & 1 & 0 \end{pmatrix}.$$

Orduan, φ-ren faktore aldagaitzak lortzeko, $XI_3 - C$ matrizearen Smithen forma normala kalkulatu behar dugu $\mathbb{R}[X]$-n, eraldaketa elementalak aplikatuz:

$$\begin{pmatrix} X-1 & 0 & -1 \\ 0 & X+1 & 1 \\ 1 & -1 & X \end{pmatrix} \xrightarrow{E_1 \leftrightarrow E_3} \begin{pmatrix} 1 & -1 & X \\ 0 & X+1 & 1 \\ X-1 & 0 & -1 \end{pmatrix}$$

$$\xrightarrow[Z_3 \to Z_3 - XZ_1]{Z_2 \to Z_2 + Z_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & X+1 & 1 \\ X-1 & X-1 & -X^2+X-1 \end{pmatrix}$$

$$\xrightarrow{E_3 \to E_3 - (X-1)E_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & X+1 & 1 \\ 0 & X-1 & -X^2+X-1 \end{pmatrix}$$

$$\xrightarrow{Z_3 \leftrightarrow Z_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & X+1 \\ 0 & -X^2+X-1 & X-1 \end{pmatrix}$$

$$\xrightarrow{Z_3 \to Z_3 - (X+1)Z_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -X^2+X-1 & X^3+X \end{pmatrix}$$

$$\xrightarrow{E_3 \to E_3 + (X^2-X+1)E_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & X^3+X \end{pmatrix}.$$

Beraz, φ-ren faktore aldagaitzak 1, 1 eta $X^3 + X$ dira. Azken teorema aplikatuz, hau da φ-ren forma kanoniko arrazionala:

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Ohartu φ-ri ezin zaiola Jordanen matrize bat elkartu, haren polinomio karakteristikoa $X^3 + X = X(X^2 + 1)$ baita, ez dena banatzen $\mathbb{R}$-ren gainean.

Matrize karratuen forma kanoniko arrazionalari buruz ere hitz egin daiteke, hurrengo teoreman erakusten dugun bezala. Gogoratu $C_1, C_2 \in M_n(K)$ bi matrize

antzekoak direla existitzen bada $P \in GL_n(K)$ non $P^{-1}C_1P = C_2$ baita. (Hemen K gorputza da.)

7.25. Teorema. *Izan bitez K gorputza eta $C \in M_n(K)$. Orduan (7.7)-koa bezalako matrize bakar bat dago C-ren antzekoa dena. Hori C-ren* forma kanoniko arrazionala *dela esaten dugu.*

FROGA. Hartu V bektore-espazioa K-ren gainean, $\dim V = n$ izanik, aukeratu $\mathcal{B}$ V-ren oinarri bat, eta definitu $\varphi : V \longrightarrow V$ aplikazio lineala $M_{\mathcal{B}}(\varphi) = C$ den moduan. (Adibidez, $V = K^n$ har daiteke eta $\mathcal{B}$, K^n-ren oinarri kanonikoa.) Orduan, matrize elkartuen propietateengatik, baliokideak dira:

(i) D matrizea φ-ri elkartuta dago.
(ii) C eta D antzekoak dira.

Orduan, φ-ri (7.7)-koa bezalako matrize bakar bat elkartu dakiokeenez, gauza bera gertatzen da C-ren antzekoak diren matrizeekin. □

Bukatzeko, eman dezagun forma kanoniko arrazionalaren aplikazio bat. Jordanen forma kanonikoa ikasten denean, emaitza hau ikusten da: C_1 eta C_2 matrizeei Jordanen matrize bat elkartu badakieke (hau da, matrize horien polinomio karakteristikoa banatzen bada K gorputzaren gainean), orduan C_1 eta C_2 antzekoak dira baldin eta soilik baldin Jordanen forma kanoniko bera badute. Konparatu hurrengo teoremarekin.

7.26. Teorema. *Izan bitez K gorputza eta $C_1, C_2 \in M_n(K)$. Orduan, baliokideak dira:*

(i) *C_1 eta C_2 antzekoak dira.*
(ii) *C_1-ek eta C_2-k faktore aldagaitz berak dituzte.*
(iii) *C_1-ek eta C_2-k forma kanoniko arrazional bera dute.*

FROGA. Izan bitez D_1 eta D_2 C_1-en eta C_2-ren forma kanoniko arrazionalak, hurrenez hurren. Orduan, C_2 eta D_2 antzekoak dira eta, hortaz, C_1 eta C_2 antzekoak dira baldin eta soilik baldin C_1 eta D_2 antzekoak badira. Matrize baten forma kanoniko arrazionalaren bakartasunarengatik, hori gertatuko da baldin eta soilik baldin D_1 eta D_2 berdinak badira. □